

#5

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

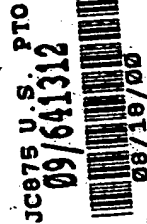
1999年 8月26日

出 願 番 号
Application Number:

平成11年特許願第239205号

出 願 人
Applicant(s):

ソニー株式会社

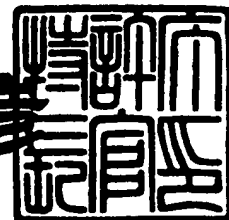


CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月29日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3052228

【書類名】 特許願

【整理番号】 9900529807

【提出日】 平成11年 8月26日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/14

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 石黒 隆二

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 海老原 宗毅

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

 【予納台帳番号】 032089

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

特平 1 1 - 2 3 9 2 0 5

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体

【特許請求の範囲】

【請求項 1】 第 1 のデータおよび前記第 1 のデータの利用の制限を記述する第 2 のデータが記録されている記録媒体を駆動して、前記第 1 のデータを受信装置に送信する送信装置において、

前記第 2 のデータの暗号値を記憶する記憶手段と、

前記受信装置を認証する場合、前記受信装置に前記第 2 のデータを送信するとともに、前記受信装置から前記第 2 のデータの暗号値を受信する通信手段と、

前記受信装置を認証する場合、前記通信手段が受信した前記第 2 のデータの暗号値と、前記記憶手段が記憶している前記第 2 のデータの暗号値との一致を判定する判定手段と

を含むことを特徴とする送信装置。

【請求項 2】 前記記憶手段は、認証以外の処理において、前記第 2 のデータの暗号値の書き込みまたは読み出しを禁止する

ことを特徴とする請求項 1 に記載の送信装置。

【請求項 3】 前記記憶手段は、耐タンパー性を有する

ことを特徴とする請求項 1 に記載の送信装置。

【請求項 4】 第 1 のデータおよび前記第 1 のデータの利用の制限を記述する第 2 のデータが記録されている記録媒体を駆動して、前記第 1 のデータを受信装置に送信する送信装置の送信方法において、

前記第 2 のデータの暗号値を記憶する記憶ステップと、

前記受信装置を認証する場合、前記受信装置に前記第 2 のデータを送信するとともに、前記受信装置から前記第 2 のデータの暗号値を受信する通信ステップと

前記受信装置を認証する場合、前記通信ステップの処理で受信した前記第 2 のデータの暗号値と、前記記憶ステップの処理で記憶している前記第 2 のデータの暗号値との一致を判定する判定ステップと

を含むことを特徴とする送信方法。

【請求項 5】 第 1 のデータおよび前記第 1 のデータの利用の制限を記述する第 2 のデータが記録されている記録媒体を駆動して、前記第 1 のデータを受信装置に送信する送信処理用のプログラムであって、

前記第 2 のデータの暗号値を記憶する記憶ステップと、

前記受信装置を認証する場合、前記受信装置に前記第 2 のデータを送信するとともに、前記受信装置から前記第 2 のデータの暗号値を受信する通信ステップと

前記受信装置を認証する場合、前記通信ステップの処理で受信した前記第 2 のデータの暗号値と、前記記憶ステップの処理で記憶している前記第 2 のデータの暗号値との一致を判定する判定ステップと

からなることを特徴とするプログラムを送信装置に実行させるプログラム格納媒体。

【請求項 6】 送信装置が送信した第 1 のデータを受信する受信装置において、

前記送信装置を認証する場合、前記送信装置から第 1 のデータの利用の制限を記述する第 2 のデータを受信するとともに、前記送信装置に前記第 2 のデータの暗号値を送信する通信手段と、

前記送信装置を認証する場合、前記通信手段が受信した第 2 のデータを基に、前記第 2 のデータの暗号値を生成する暗号値生成手段と

を含むことを特徴とする受信装置。

【請求項 7】 所定のビット数の乱数を生成する乱数生成手段を更に含み、前記通信手段は、前記送信装置に、前記乱数生成手段が生成した前記乱数とともに、前記第 2 のデータの暗号値を送信する

ことを特徴とする請求項 6 に記載の受信装置。

【請求項 8】 前記通信手段が受信した前記第 2 のデータを基に、前記第 1 のデータの受信後の前記第 1 のデータの利用の制限を記述する第 3 のデータを生成する利用制限データ生成手段を更に含み、

前記暗号値生成手段は、前記利用制限データ生成手段が生成した前記第 3 のデ

ータの暗号値を更に生成し、

前記通信手段は、前記送信装置に、前記第 3 のデータの暗号値とともに、前記第 2 のデータの暗号値を送信する

ことを特徴とする請求項 6 に記載の受信装置。

【請求項 9】 送信装置が送信した第 1 のデータを受信する受信装置の受信方法において、

前記送信装置を認証する場合、前記送信装置から第 1 のデータの利用の制限を記述する第 2 のデータを受信するとともに、前記送信装置に前記第 2 のデータの暗号値を送信する通信ステップと、

前記送信装置を認証する場合、前記通信ステップの処理で受信した第 2 のデータを基に、前記第 2 のデータの暗号値を生成する暗号値生成ステップと

を含むことを特徴とする受信方法。

【請求項 1 0】 送信装置が送信した第 1 のデータを受信する受信処理用のプログラムであって、

前記送信装置を認証する場合、前記送信装置から第 1 のデータの利用の制限を記述する第 2 のデータを受信するとともに、前記送信装置に前記第 2 のデータの暗号値を送信する通信ステップと、

前記送信装置を認証する場合、前記通信ステップの処理で受信した第 2 のデータを基に、前記第 2 のデータの暗号値を生成する暗号値生成ステップと

からなることを特徴とするプログラムを受信装置に実行させるプログラム格納媒体。

【請求項 1 1】 第 1 のデータおよび前記第 1 のデータの利用の制限を記述する第 2 のデータが記録されている記録媒体を駆動して、前記第 1 のデータを送信する送信装置、および前記第 1 のデータを受信する受信装置からなる通信システムにおいて、

前記送信装置は、

前記第 2 のデータの暗号値を記憶する記憶手段と、

前記受信装置を認証する場合、前記受信装置に前記第 2 のデータを送信するとともに、前記受信装置から前記第 2 のデータの暗号値を受信する第 1 の通信手

段と、

前記受信装置を認証する場合、前記第 1 の通信手段が受信した前記第 2 のデータの暗号値と、前記記憶手段が記憶している前記第 2 のデータの暗号値との一致を判定する判定手段と

を含み、

前記受信装置は、

前記送信装置を認証する場合、前記送信装置から前記第 2 のデータを受信するとともに、前記送信装置に前記第 2 のデータの暗号値を送信する第 2 の通信手段と、

前記送信装置を認証する場合、前記第 2 の通信手段が受信した第 2 のデータを基に、前記第 2 のデータの暗号値を生成する暗号値生成手段と

を含むことを特徴とする通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体に関し、特に、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようにした送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】

画像または音声などのコンテンツデータ、またはコンピュータプログラムなどを使用者に提供する提供者は、これらのコンテンツデータなどが無制限にコピーされて利用されることを防止するため、これらのコンテンツデータなどを予め暗号化して使用者に提供することがある。

【0003】

このような場合において、所定の暗号鍵を有する正当な使用者だけが、暗号化されているコンテンツデータなどを利用できる。

【0004】

また、コンテンツデータなどの不正な利用を、より強力に防止するため、一部の装置は、コンテンツデータなどを再生する装置とコンテンツデータなどを記録している記録媒体を駆動する装置とを相互認証させるなどの方法が採用する。

【0 0 0 5】

更に、提供者がコンテンツデータなどの利用の回数を制限したいとき、提供者は、コンテンツデータなどとともにコンテンツデータなどの利用の回数を管理するためのデータを記録媒体に記録して、提供する場合がある。この場合、記録媒体を駆動する装置は、記録媒体に記録されているコンテンツデータなどを読み出すとき、コンテンツデータなどの利用の回数を管理するためのデータを基に、コンテンツデータなどを読み出す回数が予め設定されている回数を越えるか否かを判定して、コンテンツデータなどを読み出す回数が予め設定されている回数を越えたとき、コンテンツデータなどの利用を禁止する。

【0 0 0 6】

【発明が解決しようとする課題】

しかしながら、コンテンツデータなどと共に、利用の回数を管理するためのデータを他の記録媒体にバックアップして、そのコンテンツデータなどを利用した後、バックアップされた利用の回数を管理するためのデータを元の記録媒体に戻せば、利用者は、無制限にコンテンツデータなどを利用することができる。

【0 0 0 7】

同様に、そのコンテンツデータなどを他の記録媒体に移動するとき、予め、コンテンツデータなどと共に、利用の回数を管理するためのデータを更に他の記録媒体にバックアップして、そのコンテンツデータなどを他の記録媒体に移動した後、更に他の記録媒体からコンテンツデータなどと共に、利用の回数を管理するためのデータを元の記録媒体に戻せば、利用者は、無制限にコンテンツデータなどを複製することができる。

【0 0 0 8】

コンテンツデータなどの他の記録媒体への移動の処理における、コンテンツデータなどまたは利用の回数を管理するためのデータの削除の処理を妨害しても、同様に、無制限なコンテンツデータなどの複製が可能になり、利用者は、無制限

にコンテンツデータなどを利用することができる。

【0009】

本発明はこのような状況に鑑みてなされたものであり、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようにすることを目的とする。

【0010】

【課題を解決するための手段】

請求項 1 に記載の送信装置は、第 2 のデータの暗号値を記憶する記憶手段と、受信装置を認証する場合、受信装置に第 2 のデータを送信するとともに、受信装置から第 2 のデータの暗号値を受信する通信手段と、受信装置を認証する場合、通信手段が受信した第 2 のデータの暗号値と、記憶手段が記憶している第 2 のデータの暗号値との一致を判定する判定手段とを含むことを特徴とする。

【0011】

記憶手段は、認証以外の処理において、第 2 のデータの暗号値の書き込みまたは読み出しを禁止するようにすることができる。

【0012】

記憶手段は、耐タンパー性を有するようにすることができる。

【0013】

請求項 4 に記載の送信方法は、第 2 のデータの暗号値を記憶する記憶ステップと、受信装置を認証する場合、受信装置に第 2 のデータを送信するとともに、受信装置から第 2 のデータの暗号値を受信する通信ステップと、受信装置を認証する場合、通信ステップの処理で受信した第 2 のデータの暗号値と、記憶ステップの処理で記憶している第 2 のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする。

【0014】

請求項 5 に記載のプログラム格納媒体のプログラムは、第 2 のデータの暗号値の記憶を制御する記憶制御ステップと、受信装置を認証する場合、受信装置に第 2 のデータを送信するとともに、受信装置から第 2 のデータの暗号値を受信する通信ステップと、受信装置を認証する場合、通信ステップの処理で受信した第 2

のデータの暗号値と、記憶制御ステップの処理で記憶している第 2 のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする。

【0 0 1 5】

請求項 6 に記載の受信装置は、送信装置を認証する場合、送信装置から第 1 のデータの利用の制限を記述する第 2 のデータを受信するとともに、送信装置に第 2 のデータの暗号値を送信する通信手段と、送信装置を認証する場合、通信手段が受信した第 2 のデータを基に、第 2 のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする。

【0 0 1 6】

受信装置は、所定のビット数の乱数を生成する乱数生成手段を更に設け、通信手段は、送信装置に、乱数生成手段が生成した乱数とともに、第 2 のデータの暗号値を送信するようにすることができる。

【0 0 1 7】

受信装置は、通信手段が受信した第 2 のデータを基に、第 1 のデータの受信後の第 1 のデータの利用の制限を記述する第 3 のデータを生成する利用制限データ生成手段を更に設け、暗号値生成手段は、利用制限データ生成手段が生成した第 3 のデータの暗号値を更に生成し、通信手段は、送信装置に、第 3 のデータの暗号値とともに、第 2 のデータの暗号値を送信するようにすることができる。

【0 0 1 8】

請求項 9 に記載の受信方法は、送信装置を認証する場合、送信装置から第 1 のデータの利用の制限を記述する第 2 のデータを受信するとともに、送信装置に第 2 のデータの暗号値を送信する通信ステップと、送信装置を認証する場合、通信ステップの処理で受信した第 2 のデータを基に、第 2 のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする。

【0 0 1 9】

請求項 1 0 に記載のプログラム格納媒体のプログラムは、送信装置を認証する場合、送信装置から第 1 のデータの利用の制限を記述する第 2 のデータを受信するとともに、送信装置に第 2 のデータの暗号値を送信する通信ステップと、送信装置を認証する場合、通信ステップの処理で受信した第 2 のデータを基に、第 2

のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする。

【0020】

請求項11に記載の通信システムは、送信装置が、第2のデータの暗号値を記憶する記憶手段と、受信装置を認証する場合、受信装置に第2のデータを送信するとともに、受信装置から第2のデータの暗号値を受信する第1の通信手段と、受信装置を認証する場合、第1の通信手段が受信した第2のデータの暗号値と、記憶手段が記憶している第2のデータの暗号値との一致を判定する判定手段とを含み、受信装置が、送信装置を認証する場合、送信装置から第2のデータを受信するとともに、送信装置に第2のデータの暗号値を送信する第2の通信手段と、送信装置を認証する場合、第2の通信手段が受信した第2のデータを基に、第2のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする。

【0021】

請求項1に記載の送信装置、請求項4に記載の送信方法、および請求項5に記載のプログラム格納媒体においては、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるとともに、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と、記憶している第2のデータの暗号値との一致が判定される。

【0022】

請求項6に記載の受信装置、請求項9に記載の受信方法、および請求項10に記載のプログラム格納媒体においては、送信装置を認証する場合、送信装置から第1のデータの利用の制限を記述する第2のデータが受信されるとともに、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成される。

【0023】

請求項11に記載の通信システムにおいては、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるとともに、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と記憶している第2のデータの暗号値との一致が判定され、送信装置を認証する場合、送信装置から第2のデータが受信されるととも

に、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成される。

【0024】

【発明の実施の形態】

図1は、本発明に係る記録システムの一実施の形態を示す図である。パーソナルコンピュータ1は、IEEE (Institute of Electrical and Electronic Engineers) 1394の規格に基づくネットワーク4を介して、DVD (Digital Versatile Disc) ドライブ2に接続されている。

【0025】

パーソナルコンピュータ1は、DVDドライブ2からの音声または画像（動画画像または静止画像）などのデータであるコンテンツデータの供給に先立ち、DVDドライブ2と相互認証する。この相互認証の手続きにおいて、パーソナルコンピュータ1は、ネットワーク4を介して、DVDドライブ2より供給された、コンテンツデータの利用の条件等が記述されているコンテンツ管理データを受信する。パーソナルコンピュータ1は、パーソナルコンピュータ1でのコンテンツデータの利用（コンテンツの再生、またはコンテンツデータのコピーなど）に対応して、コンテンツ管理データを更新する。

【0026】

パーソナルコンピュータ1は、DVDドライブ2より受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれに、MD (Message Digest) 5などの一方向ハッシュ関数を適用して、受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれの一方向性暗号値であるハッシュ値を求める。

【0027】

受信したコンテンツ管理データのハッシュ値および更新したコンテンツ管理データのハッシュ値は、パーソナルコンピュータ1が生成した乱数と共に、DVDドライブ2に送信される。

【0028】

パーソナルコンピュータ1は、DVDドライブ2と相互認証した後、例えば、DVD

ドライブ 2 から供給された音声または画像などのデータであるコンテンツデータ（暗号化されている）およびコンテンツデータを暗号化しているコンテンツ鍵を受信して、コンテンツ鍵でコンテンツデータを復号して、復号したコンテンツデータを再生する。

【 0 0 2 9 】

DVDドライブ 2 は、相互認証の手続きにおいて、DVD 3 に記録されているコンテンツ管理データを読み出して、ネットワーク 4 を介して、パーソナルコンピュータ 1 に送信する。DVDドライブ 2 は、相互認証の手続きにおいて、パーソナルコンピュータ 1 から、コンテンツ管理データのハッシュ値、更新されたコンテンツ管理データのハッシュ値、およびパーソナルコンピュータ 1 が生成した乱数を受信する。

【 0 0 3 0 】

DVDドライブ 2 は、パーソナルコンピュータ 1 と相互認証した後、装着されているDVD 3 に記録されている音声または画像などのデータであるコンテンツデータおよびコンテンツ鍵を読み出し、ネットワーク 4 を介して、パーソナルコンピュータ 1 に供給する。

【 0 0 3 1 】

DVDドライブ 2 は、後述するメモリに、DVD 3 に記録されているコンテンツ鍵を暗号化している暗号鍵である保存鍵、およびコンテンツ管理データにハッシュ関数を適用して得られた値であるハッシュ値を記憶している。

【 0 0 3 2 】

DVD 3 は、コンテンツ鍵で暗号化されているコンテンツデータ、コンテンツデータを暗号化している暗号鍵であるコンテンツ鍵、およびコンテンツデータの利用を管理するためのコンテンツ管理データを記録している。

【 0 0 3 3 】

DVD 3 に記録されているコンテンツデータは、共通鍵暗号方式であるDES (Data Encryption Standard) またはIDEA (International Data Encryption Algorithm) などの方式で、コンテンツ鍵で暗号化されている。

【 0 0 3 4 】

DVD 3 に記録されているコンテンツデータは、コンテンツ管理データに基づき、再生の回数、他の記録媒体へのコピー、他の記録媒体への移動が管理され、これらの操作が許可される。

【 0 0 3 5 】

コンテンツ管理データは、例えば、コンテンツデータが許可されている利用の形態（例えば、コンテンツの再生、コンテンツデータのコピー、またはコンテンツデータの移動など）を示すデータ、またはコンテンツの再生若しくはコンテンツデータのコピーの回数のデータなどから構成されている。コンテンツデータが利用されると、その利用の形態に対応して、コンテンツ管理データの値は変化する。

【 0 0 3 6 】

コンテンツ鍵は、DVDドライブ 2 のメモリに記憶されている保存鍵で暗号化されている。

【 0 0 3 7 】

ネットワーク 4 は、IEEE1394 の規格に基づき、パーソナルコンピュータ 1 が出力したデータを DVD ドライブ 2 に供給するとともに、DVD ドライブ 2 が出力したデータをパーソナルコンピュータ 1 に供給する。

【 0 0 3 8 】

図 2 は、パーソナルコンピュータ 1 の構成を説明するブロック図である。CPU (Central Processing Unit) 2 1 は、各種アプリケーションプログラムや、OS (Operating System) を実際に実行する。ROM (Read-only Memory) 2 2 は、一般的には、CPU 2 1 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 2 3 は、CPU 2 1 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらは CPU バスまたはメモリバスなどから構成されるホストバス 2 4 により相互に接続されている。

【 0 0 3 9 】

ホストバス 2 4 は、ブリッジ 2 5 を介して、PCI (Peripheral Component Interconnect/Interface) バスなどの外部バス 2 6 に接続されている。

【0040】

キーボード28は、CPU21に各種の指令を入力するとき、ユーザにより操作される。マウス29は、モニタ30の画面上のポイントの指示や選択を行うとき、ユーザにより操作される。モニタ30は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 31およびFDD (Floppy Disk Drive) 32は、それぞれハードディスクまたはフロッピーディスクを駆動し、それらにCPU21によって実行するプログラムや情報を記録または再生させる。これらのキーボード28乃至FDD32は、インターフェース27に接続されており、インターフェース27は、外部バス26、ブリッジ25、およびホストバス24を介してCPU21に接続されている。

【0041】

IEEE1394インターフェースボード33は、ネットワーク4が接続され、CPU21、またはHDD31から供給されたデータを、IEEE1394に規定されている方式の packets に格納して、ネットワーク4を介して、送信するとともに、ネットワーク4を介して、受信した packets に格納されているデータをCPU21、またはHDD31に出力する。IEEE1394インターフェースボード33は、また、IEEE1394の規定に基づく所定の処理を実行する。

【0042】

IEEE1394インターフェースボード33は、外部バス26、ブリッジ25、およびホストバス24を介してCPU21に接続されている。

【0043】

次に、図3のブロック図を参照して、DVDドライブ2の構成を説明する。IEEE1394インターフェース51は、ネットワーク4が接続され、記録再生部52またはメモリ53から供給されたデータを、IEEE1394に規定されている方式の packets に格納して、ネットワーク4を介して、パーソナルコンピュータ1に送信するとともに、ネットワーク4を介して、パーソナルコンピュータ1から受信した packets に格納されているデータを記録再生部52またはメモリ53に出力する。IEEE1394インターフェース51は、また、IEEE1394の規定に基づく所定の処理を

実行する。

【 0 0 4 4 】

IEEE1394インターフェース 5 1 は、また、パーソナルコンピュータ 1 と、後述する相互認証の処理を実行する。IEEE1394インターフェース 5 1 は、相互認証の処理のときのみ、メモリ 5 3 に記憶されているデータを読み出すとともに、メモリ 5 3 に所定のデータを記憶させる。

【 0 0 4 5 】

メモリ 5 3 は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニウムの層を有し、DVDドライブ 2 から取り外されたとき、単独で動作させにくくする為に、所定の限られた範囲の電圧でのみ動作するなど耐タンパー性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【 0 0 4 6 】

記録再生部 5 2 は、DVD 3 が装着され、装着されているDVD 3 に記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してIEEE1394インターフェース 5 1 に出力するとともに、装着されているDVD 3 にIEEE1394インターフェース 5 1 から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【 0 0 4 7 】

図 4 は、DVDドライブ 2 に記憶されているデータ、またはDVD 3 に記録されているデータを説明する図である。DVD 3 は、保存鍵により暗号化されているコンテンツ鍵、コンテンツ鍵により暗号化されているコンテンツデータ、およびコンテンツデータの利用の形態を管理するためのコンテンツ管理データが記録されている。

【 0 0 4 8 】

DVDドライブ 2 のメモリ 5 3 は、保存鍵、およびコンテンツ管理データに所定のハッシュ関数を適用して得られたハッシュ値を記憶している。DVDドライブ 2 のメモリ 5 3 に記憶されている保存鍵、またはコンテンツ管理データのハッシュ値は、IEEE1394インターフェース 5 1 がパーソナルコンピュータ 1 と相互認証す

るときのみ、メモリ 5 3 から読み出され、または値が更新される。

【 0 0 4 9 】

図 5 は、DVDドライブ 2 およびパーソナルコンピュータ 1 が相互認証するとき、ネットワーク 4 を介して、伝送されるデータの一部を説明する図である。コンテンツデータの利用に伴う相互認証において、パーソナルコンピュータ 1 は、所定のビット数の乱数（例えば、6 4 ビット）を生成するとともに、DVDドライブ 2 から受信した現在のコンテンツ管理データに対して、コンテンツデータの利用に対応する変更を加えて更新し、更新後のコンテンツ管理データを生成する。

【 0 0 5 0 】

パーソナルコンピュータ 1 は、DVDドライブ 2 から受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれに、MD 5 などの一方向ハッシュ関数を適用して、受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれの一方向性暗号値であるハッシュ値を求める。

【 0 0 5 1 】

パーソナルコンピュータ 1 は、生成した乱数、現在のコンテンツ管理データのハッシュ値、および更新後のコンテンツ管理データのハッシュ値を、DVDドライブ 2 に送信する。

【 0 0 5 2 】

パーソナルコンピュータ 1 が生成した乱数、現在のコンテンツ管理データのハッシュ値、およびパーソナルコンピュータ 1 が更新したコンテンツ管理データのハッシュ値を受信したDVDドライブ 2 は、パーソナルコンピュータ 1 が生成した乱数、現在のコンテンツ管理データ、および更新されたコンテンツ管理データのそれぞれを暗号化する。

【 0 0 5 3 】

DVDドライブ 2 は、暗号化したパーソナルコンピュータ 1 が生成した乱数、暗号化した現在のコンテンツ管理データのハッシュ値、および暗号化した更新されたコンテンツ管理データのハッシュ値を、パーソナルコンピュータ 1 に送信する。

【 0 0 5 4 】

DVDドライブ2は、所定のビット数の乱数（例えば、64ビット）を生成して、パーソナルコンピュータ1に送信する。

【0055】

パーソナルコンピュータ1は、DVDドライブ2から送信された所定のビット数の乱数を暗号化して、DVDドライブ2に送信する。

【0056】

次に、本発明に係る記録システムのコンテンツの再生の処理を、図6のフローチャートを参照して説明する。ステップS11において、パーソナルコンピュータ1およびDVDドライブ2は、相互認証して、共通鍵を生成する。相互認証の処理の詳細は、図7のフローチャートを参照して後述する。ステップS12において、DVDドライブ2のIEEE1394インターフェース51は、メモリ53に記憶されている保存鍵を読み出し、記録再生部52に、装着されているDVD3からコンテンツ鍵を読み出させる。メモリ53に記憶されている保存鍵を読み出す処理は、ステップS11の相互認証の処理で実行してもよい。DVDドライブ2のIEEE1394インターフェース51は、コンテンツ鍵を保存鍵で復号する。

【0057】

ステップS13において、DVDドライブ2のIEEE1394インターフェース51は、ステップS11で生成された共通鍵で、コンテンツ鍵を暗号化する。ステップS14において、DVDドライブ2のIEEE1394インターフェース51は、ネットワーク4を介して、共通鍵で暗号化されたコンテンツ鍵をパーソナルコンピュータ1に送信する。

【0058】

ステップS15において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ネットワーク4を介して、DVDドライブ2から送信された、共通鍵で暗号化されたコンテンツ鍵を受信する。ステップS16において、DVDドライブ2のIEEE1394インターフェース51は、記録再生部52に、装着されているDVD3から、コンテンツ鍵で暗号化されているコンテンツデータを読み出させる。DVDドライブ2のIEEE1394インターフェース51は、ネットワーク4を介して、コンテンツ鍵で暗号化されているコンテンツデータをパーソナルコンピュ

ータ 1 に送信する。

【 0 0 5 9 】

ステップ S 1 7 において、パーソナルコンピュータ 1 の IEEE1394 インターフェースボード 3 3 は、DVD ドライブ 2 から送信された、コンテンツ鍵で暗号化されているコンテンツデータを受信する。ステップ S 1 8 において、パーソナルコンピュータ 1 の CPU 2 1 は、ステップ S 1 5 で受信したコンテンツ鍵を、ステップ S 1 1 で生成した共通鍵で復号する。

【 0 0 6 0 】

ステップ S 1 9 は、パーソナルコンピュータ 1 の CPU 2 1 は、復号したコンテンツ鍵で、ステップ S 1 7 で受信したコンテンツデータを復号する。

【 0 0 6 1 】

ステップ S 2 0 において、パーソナルコンピュータ 1 の IEEE1394 インターフェースボード 3 3 は、ステップ S 1 1 の相互認証の処理で更新されたコンテンツ管理データを、ネットワーク 4 を介して、DVD ドライブ 2 に送信する。ステップ S 2 1 において、DVD ドライブ 2 の IEEE1394 インターフェース 5 1 は、更新されたコンテンツ管理データを、受信する。ステップ S 2 2 において、DVD ドライブ 2 の記録再生部 5 2 は、装着されている DVD 3 に更新されたコンテンツ管理データを記録させる。

【 0 0 6 2 】

ステップ S 2 3 において、パーソナルコンピュータ 1 は、復号したコンテンツデータからコンテンツを再生して、処理は終了する。

【 0 0 6 3 】

このように、パーソナルコンピュータ 1 は、DVD ドライブ 2 からコンテンツ鍵およびコンテンツデータを受信して、コンテンツを再生する。

【 0 0 6 4 】

次に、図 6 のフローチャートのステップ S 1 1 の処理に対応する、パーソナルコンピュータ 1 および DVD ドライブ 2 の相互認証の処理を、図 7 のフローチャートを参照して説明する。ステップ S 3 1 において、DVD ドライブ 2 の IEEE1394 インターフェース 5 1 は、記録再生部 5 2 に、装着されている DVD 3 からコンテン

ツ管理データを読み出させる。IEEE1394インターフェース 5 1 は、ネットワーク 4 を介して、コンテンツ管理データをパーソナルコンピュータ 1 に送信する。

【 0 0 6 5 】

ステップ S 5 1 において、パーソナルコンピュータ 1 の IEEE1394 インターフェースボード 3 3 は、ネットワーク 4 を介して、DVD ドライブ 2 から送信されたコンテンツ管理データを受信する。ステップ S 5 2 において、パーソナルコンピュータ 1 の CPU 2 1 は、DVD ドライブ 2 から受信したコンテンツ管理データに MD 5 などの一方向ハッシュ関数を適用して、コンテンツ管理データのハッシュ値 H_a を計算する。

【 0 0 6 6 】

ステップ S 5 3 において、パーソナルコンピュータ 1 の CPU 2 1 は、コンテンツの再生に対応させて、コンテンツの再生後のコンテンツ管理データを計算する。ステップ S 5 4 において、パーソナルコンピュータ 1 の CPU 2 1 は、コンテンツの再生後のコンテンツ管理データに MD 5 などのハッシュ関数を適用して、コンテンツの再生後のコンテンツ管理データのハッシュ値 H_b を計算する。

【 0 0 6 7 】

ステップ S 5 5 において、パーソナルコンピュータ 1 の CPU 2 1 は、例えば、64 ビットの乱数 R_a を生成する。ステップ S 5 6 において、パーソナルコンピュータ 1 の IEEE1394 インターフェースボード 3 3 は、ネットワーク 4 を介して、DVD ドライブ 2 に、乱数 R_a 、ハッシュ値 H_a 、およびハッシュ値 H_b を送信する。

【 0 0 6 8 】

ステップ S 3 2 において、DVD ドライブ 2 の IEEE1394 インターフェース 5 1 は、パーソナルコンピュータ 1 から送信された乱数 R_a 、ハッシュ値 H_a 、およびハッシュ値 H_b を受信する。ステップ S 3 3 において、DVD ドライブ 2 の IEEE1394 インターフェース 5 1 は、メモリ 5 3 に記憶されているコンテンツ管理データのハッシュ値と、ステップ S 3 2 で受信したハッシュ値 H_a とが一致するか否かを判定し、メモリ 5 3 に記憶されているコンテンツ管理データのハッシュ値と、ステップ S 3 2 で受信したハッシュ値 H_a とが一致しないと判定された場合、コ

ンテンツ管理データに改竄があったので、相互認証しないで、処理は終了する。

【 0 0 6 9 】

ステップ S 3 3 において、メモリ 5 3 に記憶されているコンテンツ管理データのハッシュ値と、ステップ S 3 2 で受信したハッシュ値 H a とが一致すると判定された場合、コンテンツ管理データに改竄がなかったので、ステップ S 3 4 に進み、DVDドライブ 2 のIEEE1394インターフェース 5 1 は、ステップ S 3 2 で受信した乱数 R a、ハッシュ値 H a、およびハッシュ値 H b を暗号化する。

【 0 0 7 0 】

ステップ S 3 5 において、DVDドライブ 2 のIEEE1394インターフェース 5 1 は、ネットワーク 4 を介して、暗号化した乱数 R a、暗号化したハッシュ値 H a、および暗号化したハッシュ値 H b をパーソナルコンピュータ 1 に送信する。

【 0 0 7 1 】

ステップ S 5 7 において、パーソナルコンピュータ 1 の C P U 2 1 は、乱数 R a、ハッシュ値 H a、およびハッシュ値 H b を暗号化する。

【 0 0 7 2 】

パーソナルコンピュータ 1 およびDVDドライブ 2 が共に正当である場合、ステップ S 3 4 におけるDVDドライブ 2 のIEEE1394インターフェース 5 1 の暗号化の方式および暗号鍵は、ステップ S 5 7 におけるパーソナルコンピュータ 1 の C P U 2 1 の暗号化の方式および暗号鍵と、それぞれ同一であり、パーソナルコンピュータ 1 およびDVDドライブ 2 において、同一の暗号化した乱数 R a、暗号化したハッシュ値 H a、および暗号化したハッシュ値 H b が得られる。

【 0 0 7 3 】

ステップ S 5 8 において、パーソナルコンピュータ 1 のIEEE1394インターフェースボード 3 3 は、ネットワーク 4 を介して、DVDドライブ 2 から送信された暗号化された乱数 R a、暗号化されたハッシュ値 H a、および暗号化されたハッシュ値 H b を受信する。ステップ S 5 9 において、パーソナルコンピュータ 1 の C P U 2 1 は、ステップ S 5 7 で暗号化した乱数 R a、暗号化したハッシュ値 H a、および暗号化したハッシュ値 H b のそれぞれと、ステップ S 5 8 で受信した暗号化された乱数 R a、暗号化されたハッシュ値 H a、および暗号化されたハッシュ

値 H_b のそれぞれとを比較して一致するか否かを判定し、暗号化した乱数 R_a 、暗号化したハッシュ値 H_a 、および暗号化したハッシュ値 H_b のそれぞれと、受信した暗号化された乱数 R_a 、暗号化されたハッシュ値 H_a 、および暗号化されたハッシュ値 H_b のいずれかが一致しないと判定された場合、DVDドライブ 2 は正当ではないので、DVDドライブ 2 を認証せず、処理は終了する。

【 0 0 7 4 】

ステップ S 3 6 において、DVDドライブ 2 の IEEE1394 インターフェース 5 1 は、64 ビットの乱数 R_b を生成する。ステップ S 3 7 において、DVDドライブ 2 の IEEE1394 インターフェース 5 1 は、ネットワーク 4 を介して、生成した乱数 R_b をパーソナルコンピュータ 1 に送信する。ステップ S 3 8 において、DVDドライブ 2 の IEEE1394 インターフェース 5 1 は、乱数 R_b を暗号化する。

【 0 0 7 5 】

ステップ S 5 9 において、暗号化した乱数 R_a 、ハッシュ値 H_a 、およびハッシュ値 H_b のそれぞれと、受信した暗号化された乱数 R_a 、ハッシュ値 H_a 、およびハッシュ値 H_b のそれぞれとが一致すると判定された場合、DVDドライブ 2 は正当なので、ステップ S 6 0 に進み、パーソナルコンピュータ 1 の IEEE1394 インターフェースボード 3 3 は、ネットワーク 4 を介して、DVDドライブ 2 が送信した乱数 R_b を受信する。

【 0 0 7 6 】

ステップ S 6 1 において、パーソナルコンピュータ 1 の CPU 2 1 は、ステップ S 6 0 で受信した乱数 R_b を暗号化する。パーソナルコンピュータ 1 および DVDドライブ 2 が正当である場合、ステップ S 3 8 における DVDドライブ 2 の IEEE1394 インターフェース 5 1 の暗号化の方式および暗号鍵は、ステップ S 6 1 におけるパーソナルコンピュータ 1 の CPU 2 1 の暗号化の方式および暗号鍵と、それぞれ同一であるので、暗号化された乱数の値は同一となる。

【 0 0 7 7 】

ステップ S 6 2 において、パーソナルコンピュータ 1 の IEEE1394 インターフェースボード 3 3 は、ネットワーク 4 を介して、ステップ S 6 1 で暗号化した乱数 R_b を DVDドライブ 2 に送信する。

【 0 0 7 8 】

ステップ S 3 9 において、DVDドライブ 2 の IEEE1394 インターフェース 5 1 は、ネットワーク 4 を介して、パーソナルコンピュータ 1 が送信した暗号化された乱数 R b を受信する。ステップ S 4 0 において、DVDドライブ 2 の IEEE1394 インターフェース 5 1 は、ステップ S 3 8 で暗号化した乱数 R b とステップ S 3 9 で受信した暗号化された乱数 R b とが一致するか否かを判定し、ステップ S 3 8 で暗号化した乱数 R b とステップ S 3 9 で受信した暗号化された乱数 R b とが一致しないと判定された場合、パーソナルコンピュータ 1 が正当ではないので、パーソナルコンピュータ 1 を認証しないで、処理は終了する。

【 0 0 7 9 】

ステップ S 4 0 において、ステップ S 3 8 で暗号化した乱数 R b とステップ S 3 9 で受信した暗号化された乱数 R b とが一致すると判定された場合、パーソナルコンピュータ 1 が正当なので、ステップ S 4 1 に進み、DVDドライブ 2 の IEEE1394 インターフェース 5 1 は、メモリ 5 3 に、ステップ S 3 2 で受信したハッシュ値 H b を記憶させる。

【 0 0 8 0 】

ステップ S 4 2 において、DVDドライブ 2 の IEEE1394 インターフェース 5 1 は、パーソナルコンピュータ 1 を認証したので、乱数 R a および乱数 R b から共通鍵を生成し、DVDドライブ 2 の処理は終了する。

【 0 0 8 1 】

ステップ S 6 3 において、パーソナルコンピュータ 1 の CPU 2 1 は、DVDドライブ 2 を認証したので、乱数 R a および乱数 R b から共通鍵を生成し、パーソナルコンピュータ 1 の処理は終了する。

【 0 0 8 2 】

このように、DVDドライブ 2 は、コンテンツ管理データのハッシュ値をメモリ 5 3 に記憶して、相互認証の手続きで、パーソナルコンピュータ 1 が計算したハッシュ値と比較するので、コンテンツ管理データが改竄されたとき、パーソナルコンピュータ 1 を認証しない。

【 0 0 8 3 】

DVDドライブ2は、相互認証の手続きで、受信した新たなコンテンツ管理データのハッシュ値を耐タンパ性を有するメモリ53に記憶するので、新たなコンテンツ管理データのハッシュ値の改竄が防止される。

【0084】

パーソナルコンピュータ1は、その都度生成した乱数とともに、コンテンツ管理データのハッシュ値をDVDドライブ2に送信するので、パーソナルコンピュータ1になりすました機器が、コンテンツ管理データのハッシュ値を受信して記憶し、相互認証しようとしても、相互認証は成功しない。

【0085】

なお、コンテンツデータの再生の回数が制限されていない場合など、ステップS53で計算されるコンテンツの再生後のコンテンツ管理データは、ステップS51で受信したコンテンツ管理データと同一でもよい。

【0086】

次に、記録媒体に記録されているコンテンツデータを不正なコピーを防止しつつ、他の記録媒体に移動させることができる、他の記録システムについて説明する。図8は、コンテンツデータを移動することができる、記録システムの他の実施の形態を示す図である。パーソナルコンピュータ101は、SCSI (Small Computer System Interface) を介して、MO (Magneto-Optical disk) ドライブ102およびハードディスク装置104に接続されている。

【0087】

MOドライブ102は、装着されているMO103に記録されている音声または画像のデータであるコンテンツデータを読み出し、パーソナルコンピュータ101または、ハードディスク装置104に供給する。MOドライブ102は、後述するメモリに、MO103に記録されているコンテンツ鍵を暗号化する暗号鍵である保存鍵、およびコンテンツ管理データにMD5などの一方向ハッシュ関数を適用して得られた値であるハッシュ値を記憶している。

【0088】

MO103は、暗号化されているコンテンツデータ、コンテンツデータを暗号化している暗号鍵であるコンテンツ鍵、およびコンテンツデータの利用を管理す

るためのコンテンツ管理データを記録している。

【0089】

MO103に記録されているコンテンツデータは、共通鍵暗号方式であるDESまたはIDEAなどの方式で、コンテンツ鍵で暗号化されている。

【0090】

MO103に記録されているコンテンツデータは、コンテンツ管理データに基づき、再生回数、他の記録媒体へのコピー、他の記録媒体への移動が管理され、これらの操作が許可される。

【0091】

コンテンツ管理データは、コンテンツデータが許可されている利用の形態を示すデータ、またはコンテンツの再生若しくはコンテンツデータのコピーの回数のデータなどから構成されている。コンテンツデータが利用されると、その利用の形態に対応して、コンテンツ管理データの値は変化する。

【0092】

コンテンツ鍵は、MOドライブ102のメモリに記憶されている保存鍵で暗号化されている。

【0093】

ハードディスク装置104は、内蔵されているハードディスクドライブにパーソナルコンピュータ101またはMOドライブ102から供給されたデータを記録するとともに、記録されているデータをパーソナルコンピュータ101またはMOドライブ102に供給する。

【0094】

図9は、パーソナルコンピュータ101の構成を説明するブロック図である。CPU121乃至FDD132のそれぞれは、それぞれ図2のCPU21乃至FDD32と同様であるので、その説明は省略する。

【0095】

SCSIインターフェースボード133は、所定のSCSIケーブルが接続され、CPU21、RAM123、またはHDD31から供給されたデータを、MOドライブ102またはハードディスク装置104に送信するとともに、MOドライブ102

またはハードディスク装置 104 から受信したデータを CPU 21、RAM 123、または HDD 31 に出力する。

【0096】

SCSI インターフェースボード 133 は、外部バス 126、ブリッジ 125、およびホストバス 124 を介して CPU 121 に接続されている。

【0097】

次に、図 10 のブロック図を参照して、MO ドライブ 102 の構成を説明する。SCSI インターフェース 151 は、SCSI ケーブルが接続され、記録再生部 152 またはメモリ 153 から供給されたデータを、パーソナルコンピュータ 101 またはハードディスク装置 104 に送信するとともに、パーソナルコンピュータ 101 またはハードディスク装置 104 から受信したデータを記録再生部 152 またはメモリ 153 に出力する。

【0098】

SCSI インターフェース 151 は、パーソナルコンピュータ 101 またはハードディスク装置 104 と、図 7 のフローチャートを参照して説明した相互認証の処理を実行する。SCSI インターフェース 151 は、相互認証の処理のときのみ、メモリ 153 に記憶されているデータを読み出すとともに、メモリ 153 に所定のデータを記憶させる。

【0099】

メモリ 153 は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニウム層を有し、MO ドライブ 102 から取り外されたとき、単独で動作させにくくする為に、所定の限られた範囲の電圧でのみ動作するなど耐タンパー性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【0100】

記録再生部 152 は、MO 102 が装着され、装着されている MO 102 に記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出して SCSI インターフェース 151 に出力するとともに、装着されている MO 102 に SCSI インターフェース 151 から供給されたコンテンツデータ、

コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【0101】

次に、図11のブロック図を参照して、ハードディスク装置104の構成を説明する。SCSIインターフェース161は、SCSIケーブルが接続され、ハードディスクドライブ162またはメモリ163から供給されたデータを、パーソナルコンピュータ101またはMOドライブ102に送信するとともに、パーソナルコンピュータ101またはMOドライブ102から受信したデータをハードディスクドライブ162またはメモリ163に出力する。

【0102】

SCSIインターフェース161は、パーソナルコンピュータ101またはMOドライブ102と、図7のフローチャートを参照して説明した相互認証の処理を実行する。SCSIインターフェース161は、相互認証の処理のときのみ、メモリ163に記憶されているデータを読み出すとともに、メモリ163に所定のデータを記憶させる。

【0103】

メモリ163は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニウム層を有し、ハードディスク装置104から取り外されたとき、単独で動作させにくくする為に、所定の限られた範囲の電圧でのみ動作するなど耐タンパー性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【0104】

ハードディスクドライブ162は、内蔵されているハードディスクに記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してSCSIインターフェース161に出力するとともに、内蔵されているハードディスクにSCSIインターフェース161から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【0105】

図12は、図8に示す記録システムの、MOドライブ102に装着されているMO103に記録されているコンテンツデータを、ハードディスクドライブ16

2に移動する処理を説明するフローチャートである。ステップS81において、MOドライブ102の記録再生部152は、MO103に記憶されているコンテンツ管理データを基に、移動後のコンテンツ管理データを計算する。記録再生部152は、計算した移動後のコンテンツ管理データをSCSIインターフェース151に供給する。

【0106】

ステップS82において、MOドライブ102のSCSIインターフェース151およびパーソナルコンピュータ101のSCSIインターフェースボード133は、図7のフローチャートを参照して説明した処理と同様の手続きで、相互認証して、共通鍵K1を生成する。

【0107】

ただし、ステップS31において、SCSIインターフェースボード133は、パーソナルコンピュータ101に現在のコンテンツ管理データおよび移動後のコンテンツ管理データを送信し、パーソナルコンピュータ101は、受信した現在のコンテンツ管理データおよび移動後のコンテンツ管理データを基に、ハッシュ値を計算する。

【0108】

ステップS83において、MOドライブ102のSCSIインターフェース151は、ステップS82の相互認証と同時に、メモリ153に記憶されているコンテンツ管理データをステップS81で計算した移動後の値に変更させる。

【0109】

ステップS84において、MOドライブ102のSCSIインターフェース151は、記録再生部152にMO103からコンテンツ鍵を読み出させ、メモリ153に記憶されている保存鍵でコンテンツ鍵を復号する。

【0110】

ステップS85において、MOドライブ102のSCSIインターフェース151は、復号されたコンテンツ鍵をステップS82で生成した共通鍵K1で暗号化する。ステップS86において、MOドライブ102のSCSIインターフェース151は、共通鍵K1で暗号化されたコンテンツ鍵を、パーソナルコンピュータ101

1 に送信する。

【0111】

ステップ S 8 7 において、パーソナルコンピュータ 1 0 1 の SCSI インターフェースボード 1 3 3 は、MO ドライブ 1 0 2 から送信された暗号化されているコンテンツ鍵を受信する。

【0112】

ステップ S 8 8 において、パーソナルコンピュータ 1 0 1 の CPU 1 2 1 は、ステップ S 8 7 で受信したコンテンツ鍵を、ステップ S 8 2 で生成した共通鍵 K 1 で復号する。

【0113】

ステップ S 8 9 において、ハードディスク装置 1 0 4 のハードディスクドライブ 1 6 2 は、移動後のコンテンツ管理データ（相互認証の処理に利用される）を計算する。

【0114】

ステップ S 9 0 において、ハードディスク装置 1 0 4 の SCSI インターフェース 1 6 1 およびパーソナルコンピュータ 1 0 1 の SCSI インターフェースボード 1 3 3 は、図 7 のフローチャートを参照して説明した処理と同様の手続きで、相互認証して、共通鍵 K 2 を生成する。ステップ S 9 0 のパーソナルコンピュータ 1 0 1 とハードディスク装置 1 0 4 の相互認証の処理で、パーソナルコンピュータ 1 0 1 は、ハードディスク装置 1 0 4 にステップ S 8 1 で MO ドライブ 1 0 2 が計算した移動後のコンテンツ管理データを送信する。

【0115】

ステップ S 9 1 において、ハードディスク装置 1 0 4 の SCSI インターフェース 1 6 1 は、ステップ S 9 0 の相互認証と同時に、メモリ 1 6 3 に記憶されているコンテンツ管理データを、ステップ S 9 0 で受信した移動後のコンテンツ管理データに変更させる。

【0116】

ステップ S 9 2 において、パーソナルコンピュータ 1 0 1 の CPU 1 2 1 は、ステップ S 8 8 で復号されたコンテンツ鍵を、共通鍵 K 2 で暗号化する。ステッ

ブ S 9 3 において、パーソナルコンピュータ 1 0 1 の SCSI インターフェースボード 1 3 3 は、共通鍵 K 2 で暗号化されているコンテンツ鍵をハードディスク装置 1 0 4 に送信する。

【0 1 1 7】

ステップ S 9 4 において、ハードディスク装置 1 0 4 の SCSI インターフェース 1 6 1 は、パーソナルコンピュータ 1 0 1 から送信された、共通鍵 K 2 で暗号化されているコンテンツ鍵を受信する。

【0 1 1 8】

ステップ S 9 5 において、ハードディスク装置 1 0 4 の SCSI インターフェース 1 6 1 は、ステップ S 9 4 で受信したコンテンツ鍵を共通鍵 K 2 で復号する。

【0 1 1 9】

ステップ S 9 6 において、MO ドライブ 1 0 2 の記録再生部 1 5 2 は、装着されている MO 1 0 3 からコンテンツ鍵を削除する。

【0 1 2 0】

ステップ S 9 7 において、ハードディスク装置 1 0 4 の SCSI インターフェース 1 6 1 は、ステップ S 9 5 で復号されたコンテンツ鍵を、メモリ 1 6 3 に記憶している保存鍵で暗号化する。ステップ S 9 8 において、ハードディスク装置 1 0 4 のハードディスクドライブ 1 6 2 は、暗号化されたコンテンツ鍵を記録する。

【0 1 2 1】

ステップ S 9 9 において、MO ドライブ 1 0 2 の SCSI インターフェース 1 5 1 は、記録再生部 1 5 2 に MO 1 0 3 からコンテンツデータを読み出させ、ハードディスク装置 1 0 4 にコンテンツデータを移動する。

【0 1 2 2】

このように、図 8 に示す記録システムにおいては、MO 1 0 3 に記録されているコンテンツデータをハードディスク装置 1 0 4 に移動する。MO 1 0 3 に記録されているコンテンツデータを他の MO ディスクにバックアップしておき、MO 1 0 3 に記録されているコンテンツデータを利用した後、バックアップされたコンテンツデータが記録されている MO ディスクを使用しようとしても、ステップ S 8 2 の相互認証の処理で不正と判定されるので、バックアップしたコンテンツ

データを使用することができない。

【0123】

なお、コンテンツデータが記録される記録媒体は、DVD3、MO103、またはハードディスクとして説明したが、光ディスク、半導体メモリ、磁気テープ、または印刷物（例えば、2次元バーコードが印刷された印刷物）でもよい。

【0124】

また、記録媒体に記録するコンテンツデータは、音声または画像（動画像または静止画像）として説明したが、コンピュータプログラム、所定のサーバなどへのアクセス権を記述したデータ（ファイル）、または所定のサービスを利用するためのデータを記憶したチケットなどでもよい。

【0125】

コンテンツを再生する装置は、パーソナルコンピュータ1またはパーソナルコンピュータ101として説明したが、パーソナルコンピュータ1またはパーソナルコンピュータ101に限らず、セットトップボックスなどの家庭電化製品、サーバ、またはDVDドライブなどのコンピュータ周辺装置などでもよい。

【0126】

パーソナルコンピュータ1またはパーソナルコンピュータ101が実行するコンテンツの再生の処理、相互認証の処理などのプログラムを内部が解析しにくいソフトウェアとすれば、コンテンツデータの不正使用に対する防御をより強力にすることができる。

【0127】

パーソナルコンピュータ1、パーソナルコンピュータ101、DVDドライブ2、MOドライブ102、またはハードディスク装置104は、IEEE1394の規格に基づくネットワーク4またはSCSIケーブルを介してデータを送信するとともに、受信すると説明したが、他のネットワーク、他のデータ転送用のインターフェースなどでもよい。

【0128】

例えば、半導体メモリが内蔵された、シリアル制御されるメモリカードは、コンテンツデータである、暗号化した音楽データを記憶している。音楽を再生する

とき、メモリカードは、所定のパーソナルコンピュータのインターフェースに装着される。

【0129】

音楽の再生の回数を制限するため、そのメモリカードに記憶されているコンテンツ管理データは、音楽の再生の回数に対応してデクリメントされる。コンテンツ管理データが”0”になったとき、メモリカードが装着されているパーソナルコンピュータは、メモリカードに記憶されている音楽データを利用しない（音楽を再生しない）。

【0130】

メモリカードが装着されるインターフェースが、コンテンツ管理データのハッシュ値を記憶すれば、メモリカードに記憶されているコンテンツ管理データを他のメモリカードにバックアップしても、その後に、一度でもメモリカードに記憶されている音楽データが利用されれば、バックアップされた音楽データを再生することはできない。

【0131】

例えば、メモリカードが装着されるインターフェースが相互認証の処理の際に出力する信号を監視して、その信号を記録し、またその信号を改竄しても、コンテンツ管理データのハッシュ値は、その都度生成された乱数とともに、送信されるので、相互認証を成功させることは、不可能である。

【0132】

このように、コンテンツデータが記録される記録媒体の種類、信号が送信される方式、インターフェースの種類などに拘わらず、不正な複製を防止することができる。

【0133】

なお、メモリ53、メモリ153、またはメモリ163は、コンテンツ管理データにハッシュ関数を適用して得られるハッシュ値を記憶するとして説明したが、ハッシュ値に限らず、DESなどの共通鍵暗号方式で暗号化したコンテンツ管理データを記憶してもよい。

【0134】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【0135】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図13に示すように、磁気ディスク351（フロッピディスクを含む）、光ディスク352（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク353（MD(Mini-Disc)を含む）、若しくは半導体メモリ354などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM302や、記憶部308を構成するハードディスクなどにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じてルータ、モデムなどのインタフェースを介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0136】

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0137】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0138】

【発明の効果】

請求項1に記載の送信装置、請求項4に記載の送信方法、および請求項5に記

載のプログラム格納媒体によれば、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるとともに、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と、記憶している第2のデータの暗号値との一致が判定されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【0139】

請求項6に記載の受信装置、請求項9に記載の受信方法、および請求項10に記載のプログラム格納媒体によれば、送信装置を認証する場合、送信装置から第1のデータの利用の制限を記述する第2のデータが受信されるとともに、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【0140】

請求項11に記載の通信システムによれば、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるとともに、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と、記憶している第2のデータの暗号値との一致が判定され、送信装置を認証する場合、送信装置から第2のデータが受信されるとともに、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【図面の簡単な説明】

【図1】

本発明に係る記録システムの一実施の形態を示す図である。

【図2】

パーソナルコンピュータ1の構成を説明するブロック図である。

【図 3】

DVDドライブ 2 の構成を説明するブロック図である。

【図 4】

DVDドライブ 2 に記憶されているデータ、またはDVD 3 に記録されているデータを説明する図である。

【図 5】

DVDドライブ 2 およびパーソナルコンピュータ 1 が相互認証するとき、ネットワーク 4 を介して、送信されるデータの一部を説明する図である。

【図 6】

コンテンツの再生の処理を説明するフローチャートである。

【図 7】

相互認証の処理を説明するフローチャートである。

【図 8】

記録システムの他の実施の形態を示す図である。

【図 9】

パーソナルコンピュータ 1 0 1 の構成を説明するブロック図である。

【図 1 0】

MOドライブ 1 0 2 の構成を説明するブロック図である。

【図 1 1】

ハードディスク装置 1 0 4 の構成を説明するブロック図である。

【図 1 2】

コンテンツの移動の処理を説明するフローチャートである。

【図 1 3】

プログラム格納媒体を説明する図である。

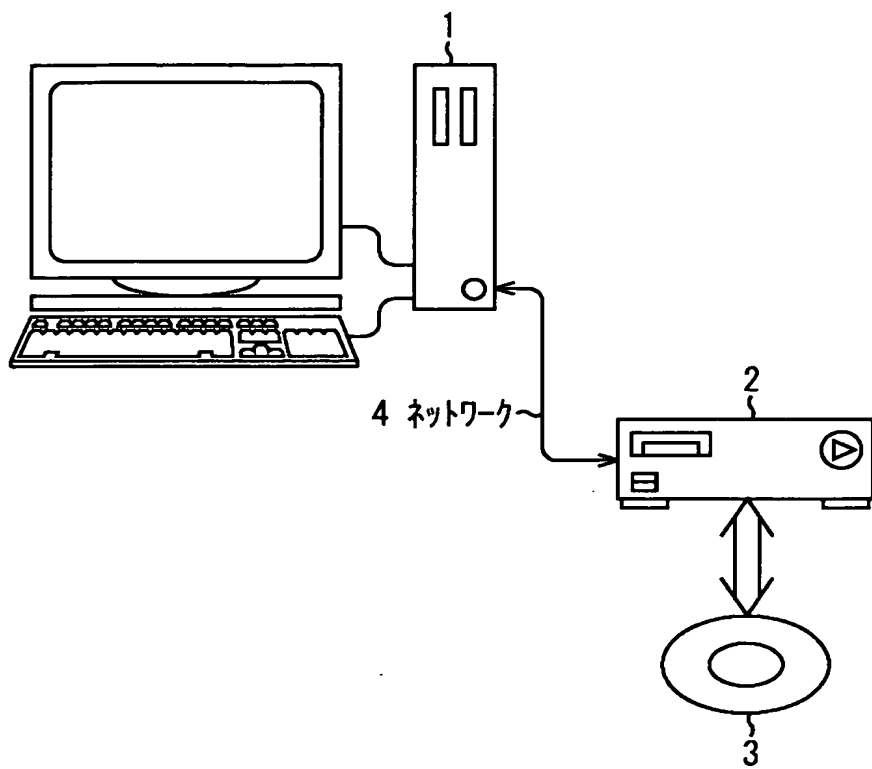
【符号の説明】

1 パーソナルコンピュータ, 2 DVDドライブ, 3 DVD, 4 ネットワーク, 2 1 CPU, 3 3 IEEE1394インターフェースボード, 5 1 IEEE1394インターフェース, 5 2 記録再生部, 5 3 メモリ, 1 0 1 パーソナルコンピュータ, 1 0 2 MOドライブ, 1 0 3 MO, 1 0 4

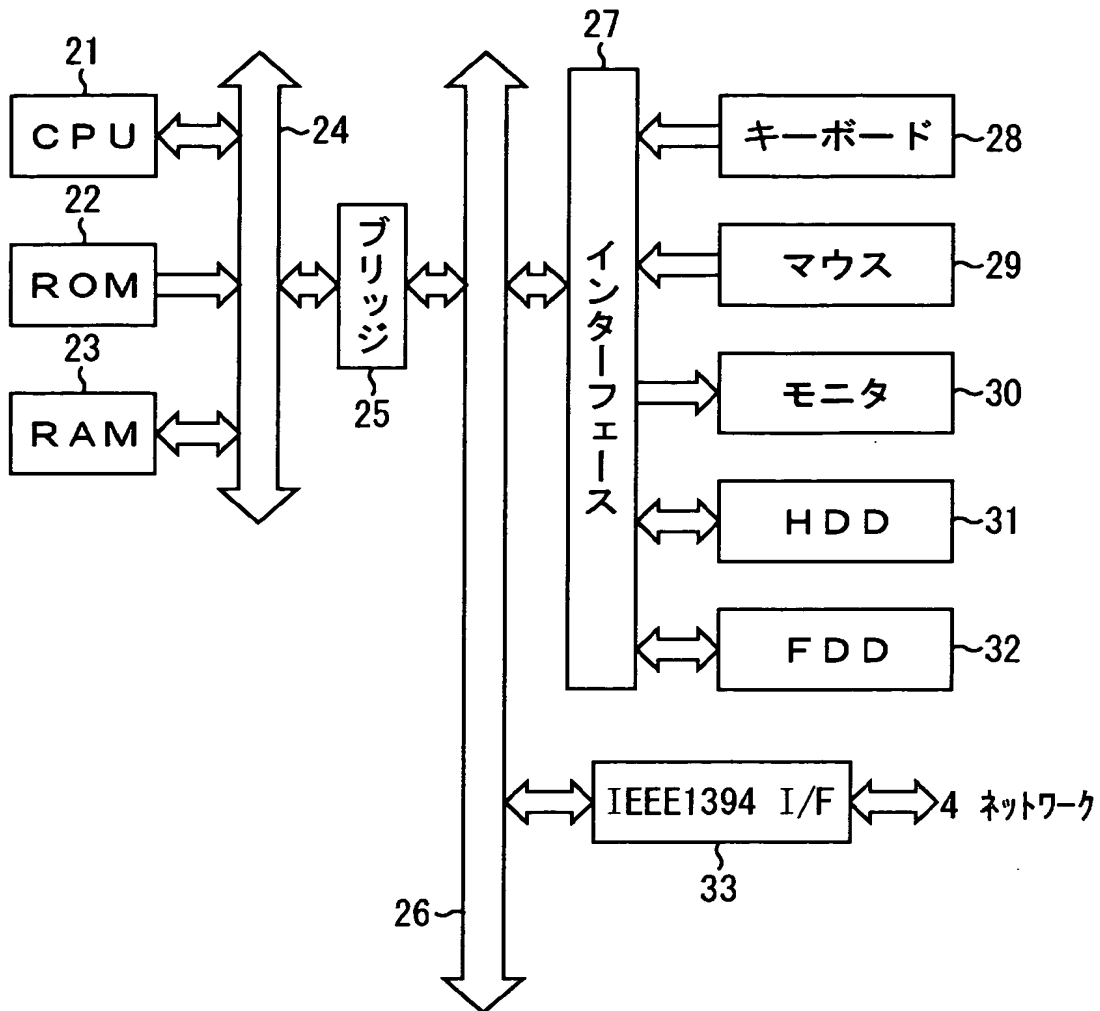
ハードディスク装置, 121 CPU, 133 SCSIインターフェースボ
ード, 151 SCSIインターフェース, 152 記録再生部, 153 メ
モリ, 161 SCSIインターフェース, 162 ハードディスクドライブ,
163 メモリ, 301 CPU, 302 ROM, 303 RAM,
308 記憶部, 351 磁気ディスク, 352 光ディスク, 353
光磁気ディスク, 354 半導体メモリ

【書類名】 図面

【図 1】

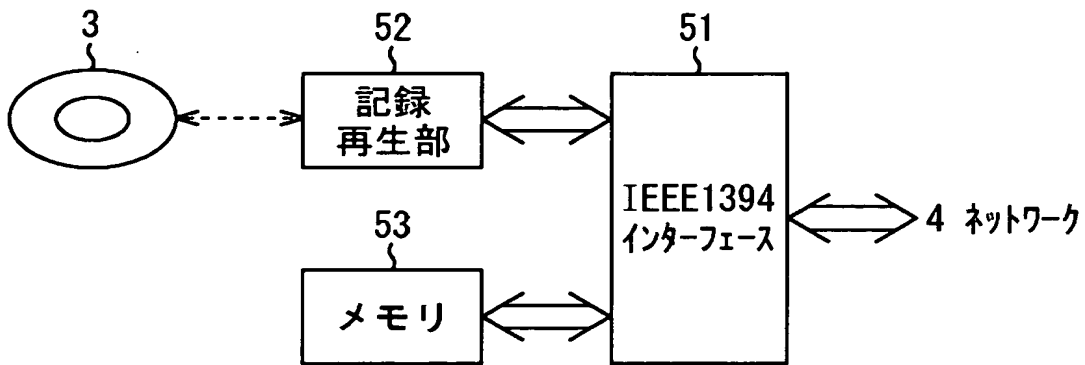


【図 2】



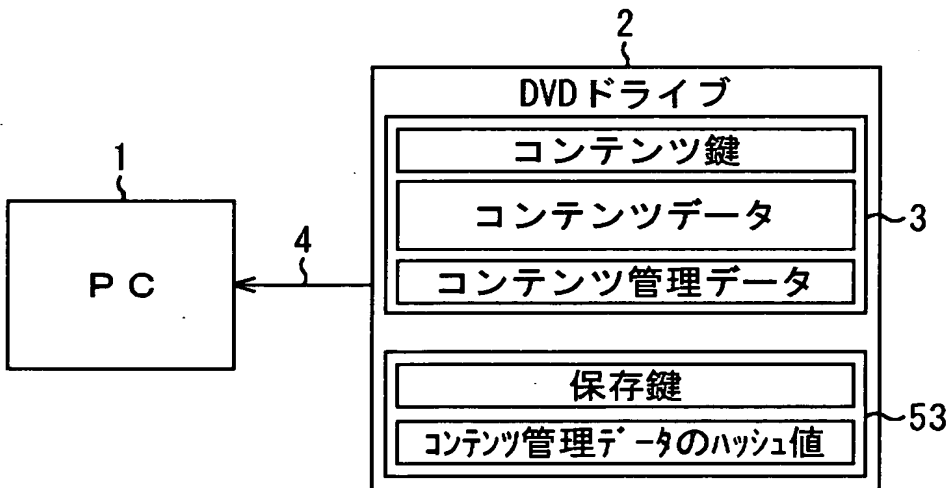
パーソナルコンピュータ 1

【図 3】

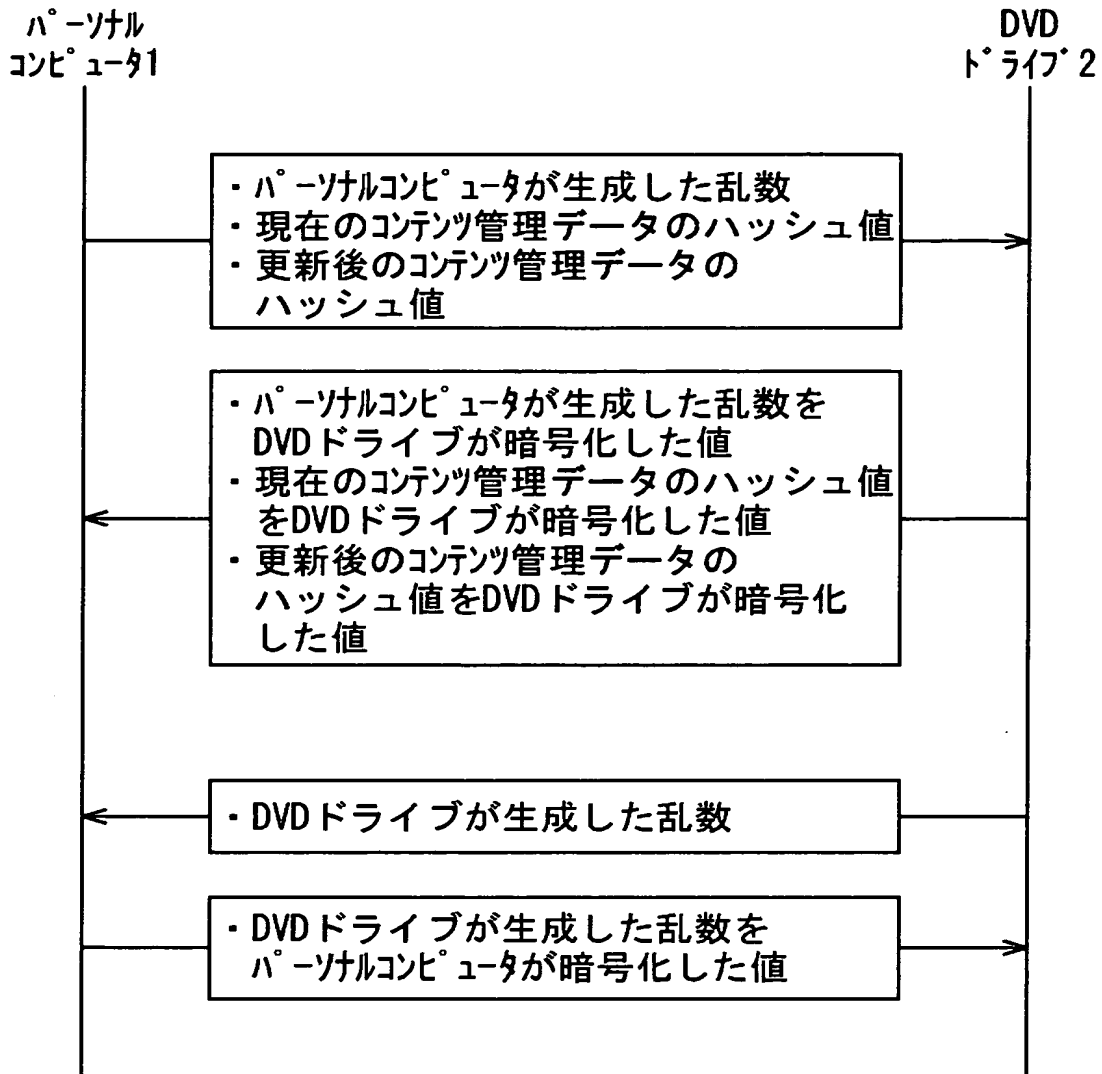


DVDドライブ 2

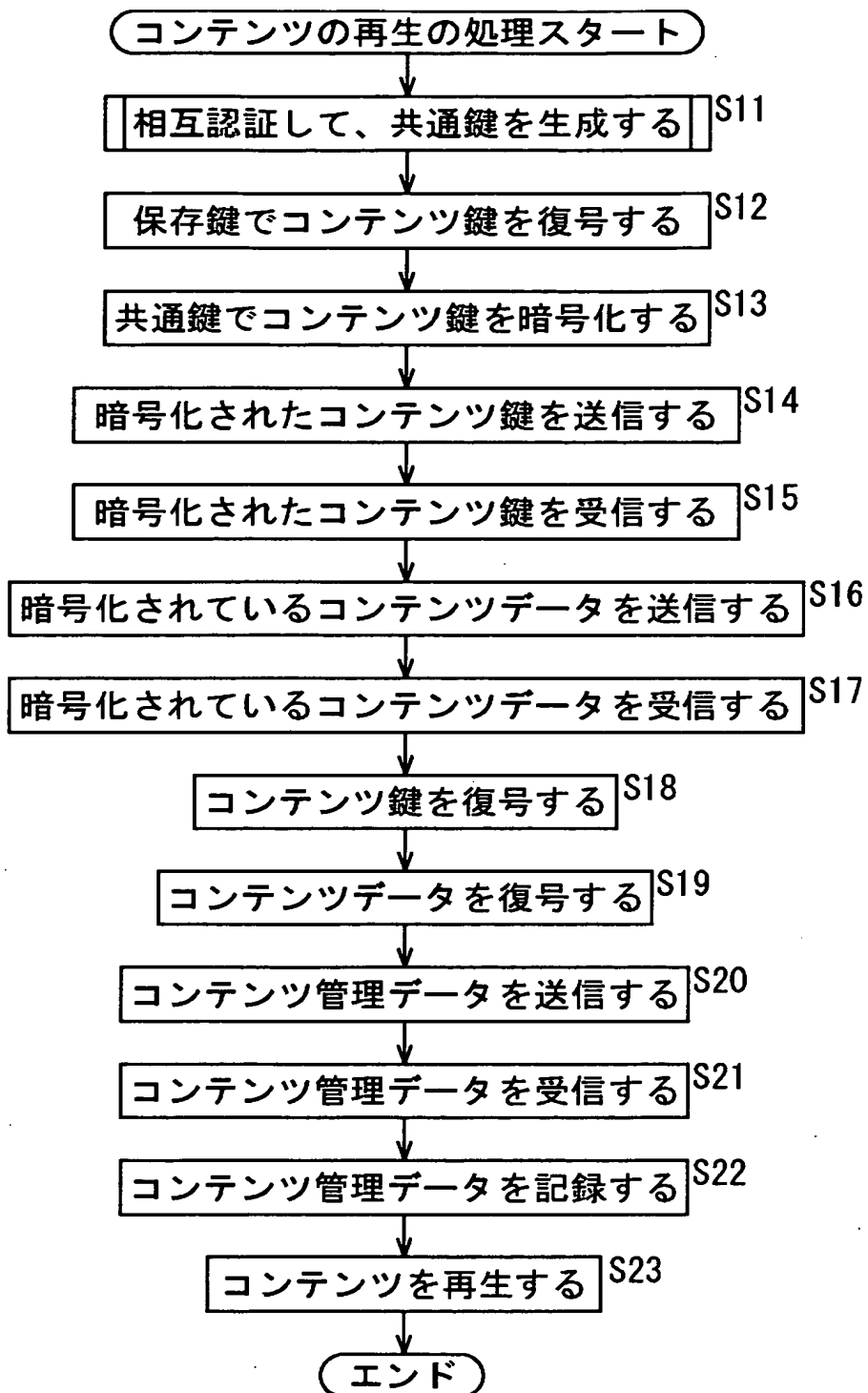
【図 4】



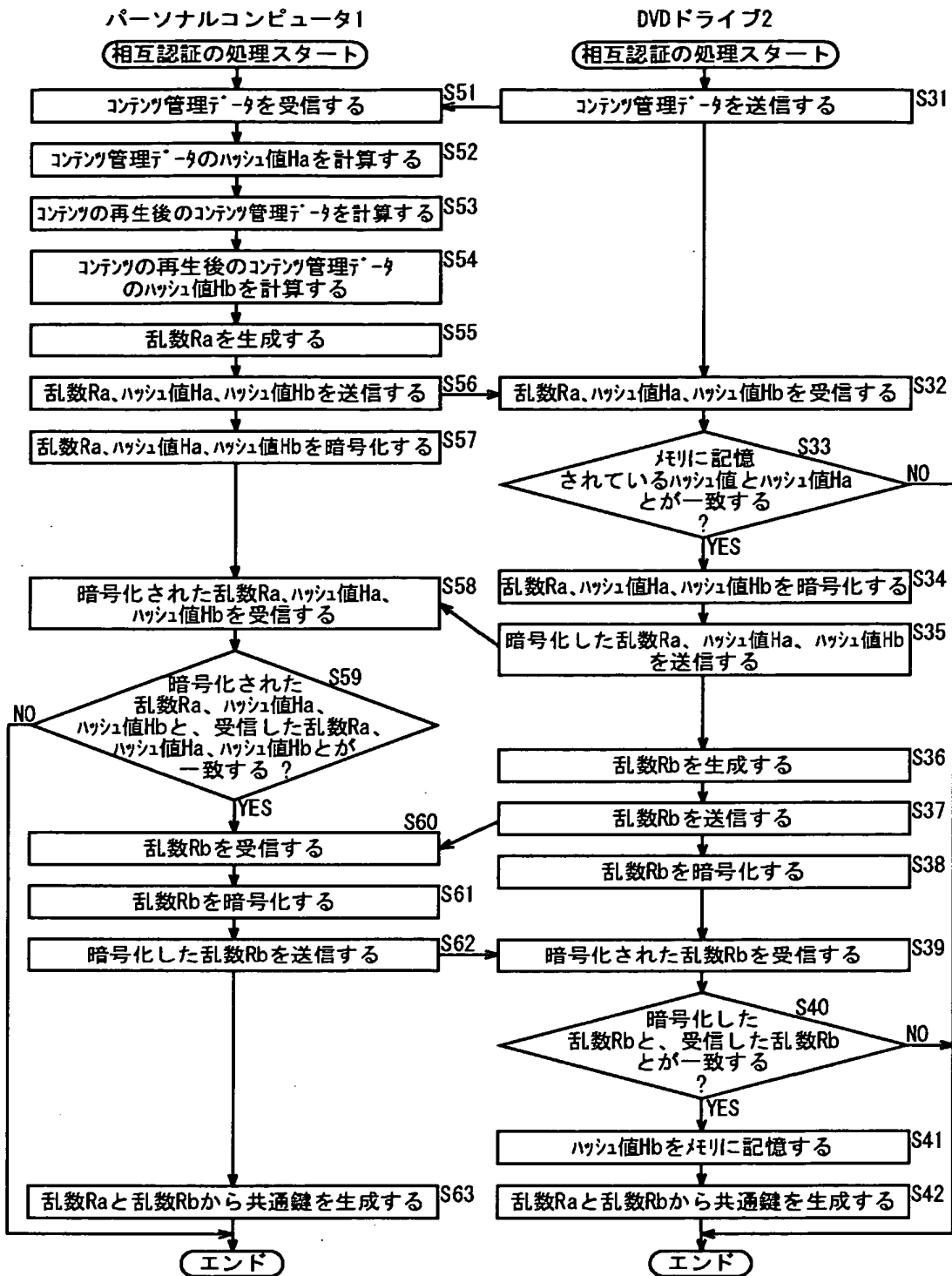
【図 5】



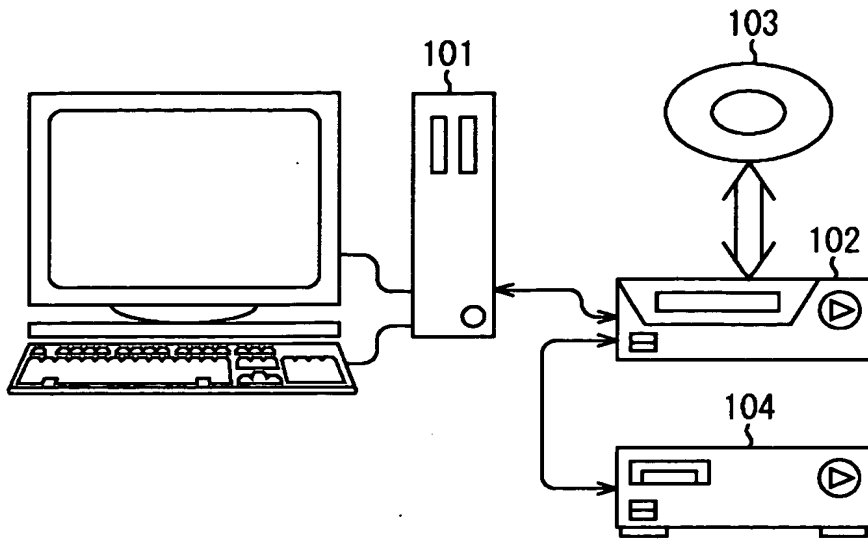
【図 6】



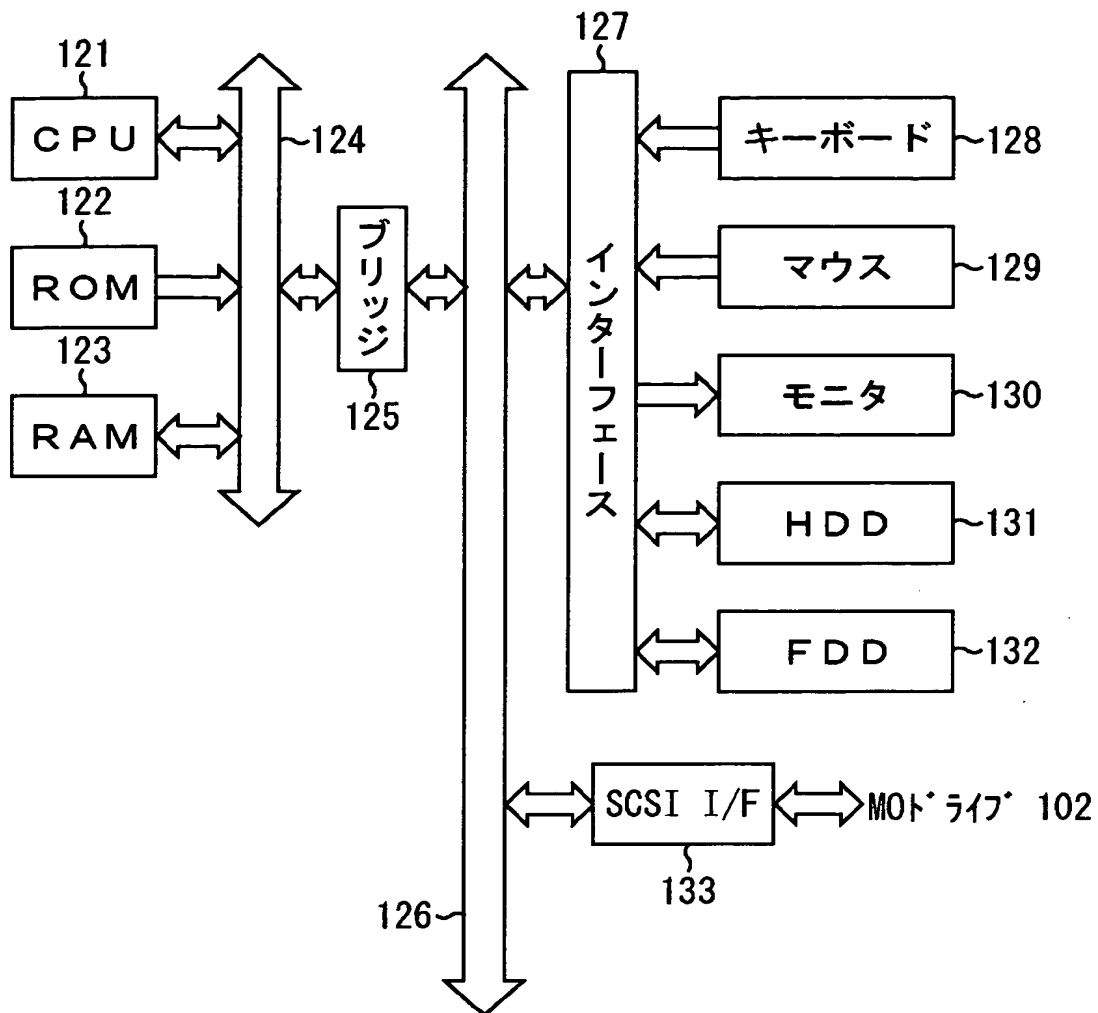
【図 7】



【図 8】

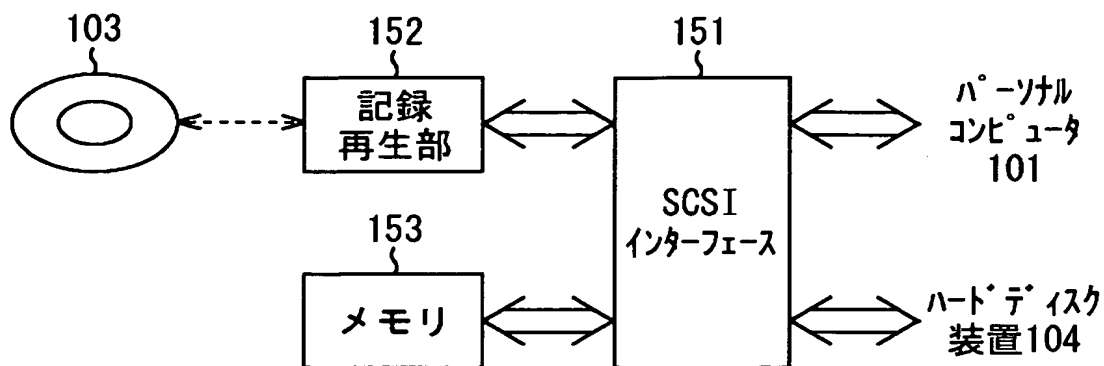


【図 9】



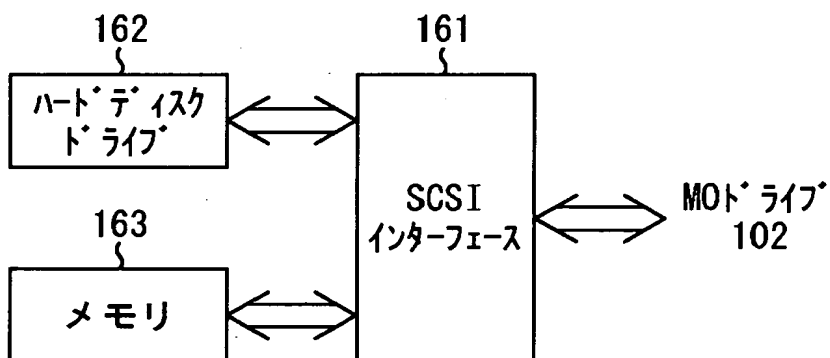
パーソナルコンピュータ 101

【図 1 0】



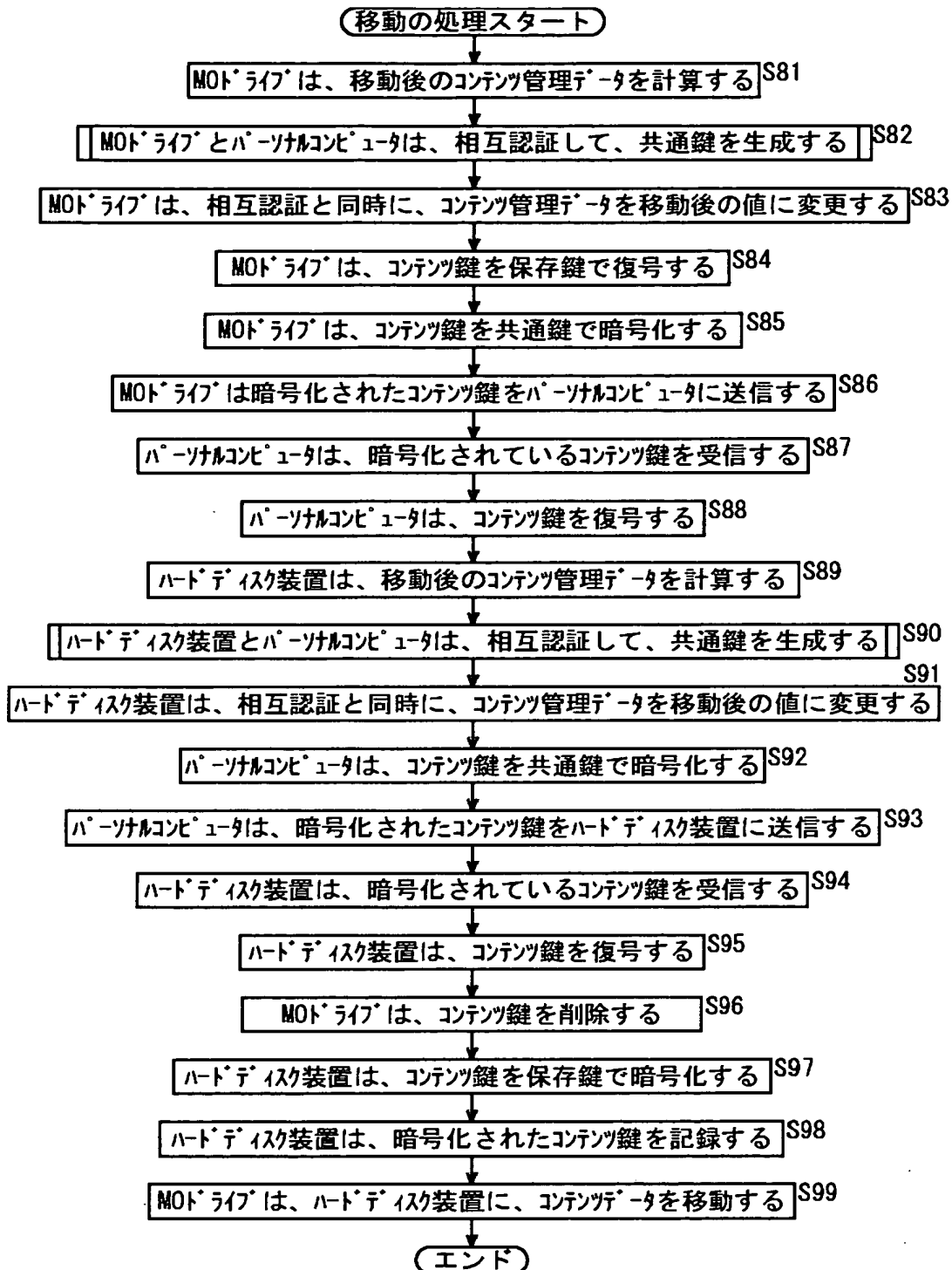
MOドライブ 102

【図 1 1】

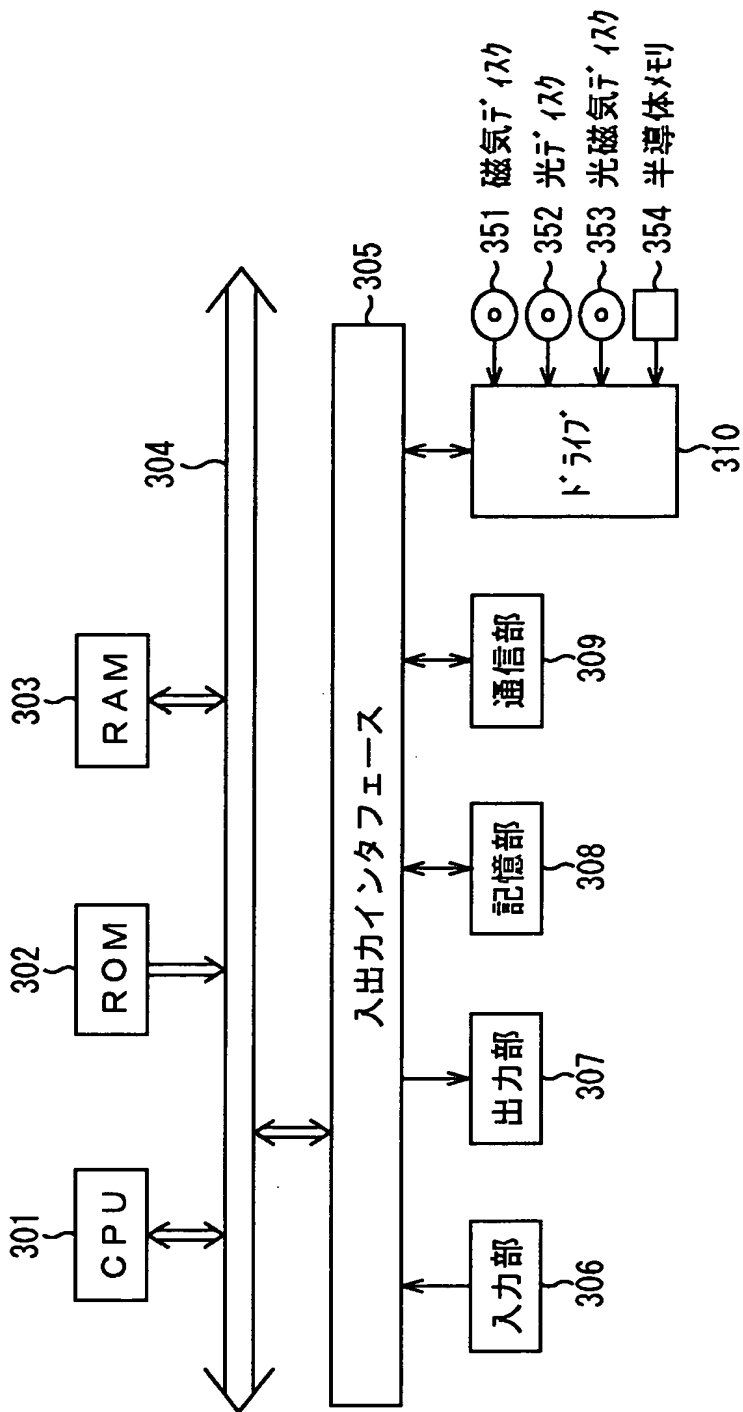


ハードディスク装置 104

【図 1 2】



【図 1 3】



パーソナルコンピュータ 1

【書類名】 要約書

【要約】

【課題】 不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限する。

【解決手段】 メモリ 53 は、コンテンツ管理データのハッシュ値を記憶する。IEEE1394 インターフェース 51 は、ネットワークを介して接続されているパーソナルコンピュータを認証するとき、パーソナルコンピュータにコンテンツ管理データを送信するとともに、パーソナルコンピュータからコンテンツ管理データのハッシュ値を受信する。IEEE1394 インターフェース 51 は、パーソナルコンピュータを認証するとき、受信したコンテンツ管理データのハッシュ値と、記憶しているコンテンツ管理データのハッシュ値との一致を判定する。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社